State of Iowa Enterprise Laptop Data Protection Standard

December 14, 2006

Purpose

This standard establishes minimum requirements for installation and operation of laptop computers for State of Iowa agencies to protect information technology (IT) resources and the data stored, processed, and transmitted by those resources; including those data that are confidential or contain personally identifiable information (PII) or personal health information (PHI).

Overview

Laptop computers can provide agencies and users benefits such as portability, flexibility, and increased productivity. Laptop computers allow users to take computers and data with them wherever they go. For some personnel, particularly those that regularly work at customer locations or are required to travel, laptop computers are an important tool.

The benefits of laptop computers, however, come with potential risks. Due to their portable nature, a significant source of risk is the loss or theft of devices and a subsequent exposure of critical information stored on those devices. Also due to their mobile nature, these devices may connect to potentially hostile environments that lack adequate protections, subjecting the devices to attacks or potential infections, which may in turn be brought back to a State of Iowa network.

Scope

This standard sets minimum requirements for encryption of laptop and tablet computers that hold state-owned data or connect to state-owned or managed networks, including those of contractors, state business partners and individuals. For the purpose of this standard, security is defined as the ability to protect the integrity, confidentiality and availability of information processed, stored and transmitted by an agency.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Laptop Standard are defined below:

- **Laptop Computer:** Laptop computers are designed to be lightweight and have the ability to operate for extended periods of time with a self-contained power source. For the purpose of this standard, a laptop computer includes devices classified as tablet computers.

- **Data Classification System:** The classification of all data stored, processed or transmitted into categories based on the extent to which they must be protected. Categories may include confidential, sensitive and public.

- **Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

- **Personally Identifiable Information:** Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.

- **Personal Health Information:** Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium

Enterprise Laptop Standard

If security controls are not in place or they are configured improperly, the use of laptop computers can expose sensitive or confidential data to access by unauthorized personnel and malicious software. Therefore, to ensure that all data is appropriately protected, the following minimum standards must be met for all laptop computers:

1. **Laptop Inventory.** Agencies will maintain an inventory of all laptop computers, to whom they are assigned and the encryption used on the laptop.

2. **Data Encryption and Authentication.** All laptop computers must be encrypted.

    - All laptop computers shall require pre-boot user authentication.
    - The entire hard drive shall be encrypted using the Advanced Encryption Standard (AES[1]) cipher using at least a 256-bit key length.
    - An audit trail shall be maintained to demonstrate, with a high degree of confidence, that a device was encrypted.
    - The encryption process and procedures shall be centrally managed at the agency and/or enterprise level.

3. **Loss/Theft Procedures.** Loss or theft of any laptop computer should be reported to the Chief Information Security Officer within 24 hours. Procedures should also be in place to change authentication credentials to any systems the device may have accessed;

[1] Prior to its adoption by NIST in 2000 with the issuance of FIPS 197, AES was commonly known as the Rijndael block cipher.

including non-state-owned as well as state-owned devices which store sensitive or confidential data.

4. **Physical Protection.** Users of laptop computers are responsible for their physical protection. Use of cable locks and other physical security devices are encouraged where appropriate.

5. **Primary Storage/Data Backups.** To ensure data availability in the event of device loss or theft, a laptop computer should not be the only or primary storage device for State of Iowa data. In the case where the laptop computer is the primary storage device, frequent and regular backups of the data must be made, according to agency policy.

6. **Client security maintained.** All laptop computers must have a properly-configured, host-based firewall, up-to-date antivirus software and be compliant with applicable enterprise and agency standards. Software patches must be applied per the agency's patching schedule.

7. **Assessment.** The ISO will periodically conduct assessments of agency compliance with this standard. Agencies will provide access to inventory information and systems as required to determine compliance. If violations of the laptop computer standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

8. **Awareness Training:** Laptop computer users shall be provided with mobile security awareness training. At a minimum, users shall be provided with documentation describing mobile computing risks.

Effective Date

Agencies must comply with this standard no later than December 31, 2007, for all laptop computers that store data classified by the agency as confidential, except, if the Iowa Legislature appropriates funds to pay the hardware and software cost of encrypting all laptops in the 2007 legislative session, then all laptops must be encrypted per this standard by December 31, 2007. Irrespective of legislative action, all laptop computers must be encrypted per this standard no later than December 31, 2008.

Enforcement

This standard will be enforced per IAC 11-25.11(8A). The Information Security Office will periodically review a random sampling of laptop or tablet computers from agencies to assure the computers are properly encrypted, or if an exception has been granted, do not contain confidential or other data requiring protection per the agency data classification.